Bitdefender®

Les ransomwares : une affaire personnelle.

Sommaire

Auteurs

Liviu Arsene – Analyste sénior en cyber-menaces
Alexandra Gheorghe - Spécialiste en cyber-sécurité

1. Introduction

Les virus biologiques mutent et tentent de s'adapter à leur environnement pour survivre. Lorsqu'ils réussissent, ils peuvent alors se répandre et provoquer des épidémies importantes. On retrouve le même comportement avec les cyber-menaces. En 2015, les ransomwares ont causé plus de 350 millions de dollars de dommages, confirmant ainsi leur statut de menace la plus prolifique de ces dernières années.

Cette étude, menée par Bitdefender en novembre 2015, se base sur un échantillon de 3009 internautes basés en France, aux États-Unis, en Allemagne, au Danemark, au Royaume-Uni et en Roumanie. Elle offre donc le point de vue d'une victime potentielle d'une perte de données suite à une infection par un crypto-ransomware. Il s'agit de définir ce qui pousse les victimes à payer. Combien valent à leurs yeux leurs données personnelles ? Quel rôle la protection antivirus joue-t-elle dans la résolution de cette équation ?

Résultats clés :

- 50% des internautes ne savent pas précisément que les ransomwares sont une menace pouvant bloquer l'accès aux données de l'ordinateur.
- La moitié des victimes sont prêtes à payer jusqu'à 450 euros pour récupérer leurs données chiffrées.
- Les documents personnels sont la principale priorité des internautes.
- Les internautes britanniques sont susceptibles de payer plus pour récupérer leurs fichiers.
- Les internautes américains sont la cible principale des ransomwares.

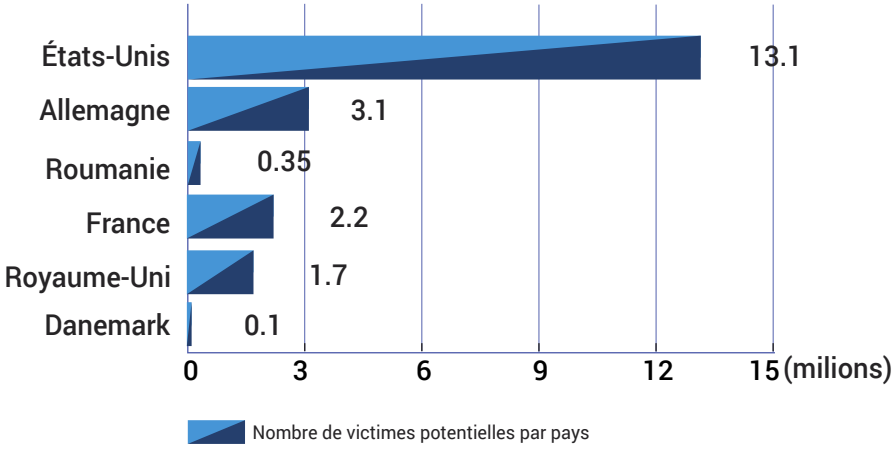
1ère PARTIE
Le point de vue des victimes

Une étude menée par Bitdefender a révélé que moins de la moitié des internautes savent précisément que les ransomwares constituent une menace bloquant l'accès aux données personnelles, tandis que deux tiers savent que les ransomwares peuvent endommager les ordinateurs. L'étude de novembre 2015 a été conduite par iSense Solutions auprès d'un total de 3009 personnes interrogées en Roumanie, aux États-Unis, au Royaume-Uni, en France, en Allemagne et au Danemark.

Ce malware, qui se base sur l'extorsion, prend pour cible tous les internautes sans discrimination, dont 4,1% de la population des États-Unis, pour un total avoisinant 13,1 millions de personnes, selon l'étude.

32% des internautes n'ayant pas été infectés pensent qu'il est très peu probable qu'ils le soient un jour.

Même si l'Allemagne, la Roumanie, la France, le Royaume-Uni et le Danemark présentent des pourcentages moins élevés[1] en termes de victimes de ransomwares – respectivement 3,8%, 3,4%, 3,3%, 2,6% et 2% – les personnes infectées se comptent tout de même par millions. L'Allemagne compte 3,1 millions de victimes potentielles, suivie par la France avec 2,2 millions, le Royaume-Uni avec 1,7 million, la Roumanie avec 350 000 et enfin 100 000 victimes potentielles au Danemark.



La moitié des victimes sont prêtes à payer jusqu'à 450 euros pour récupérer leurs données même s'il n'y a pas de garantie de recevoir la clé de déchiffrement.

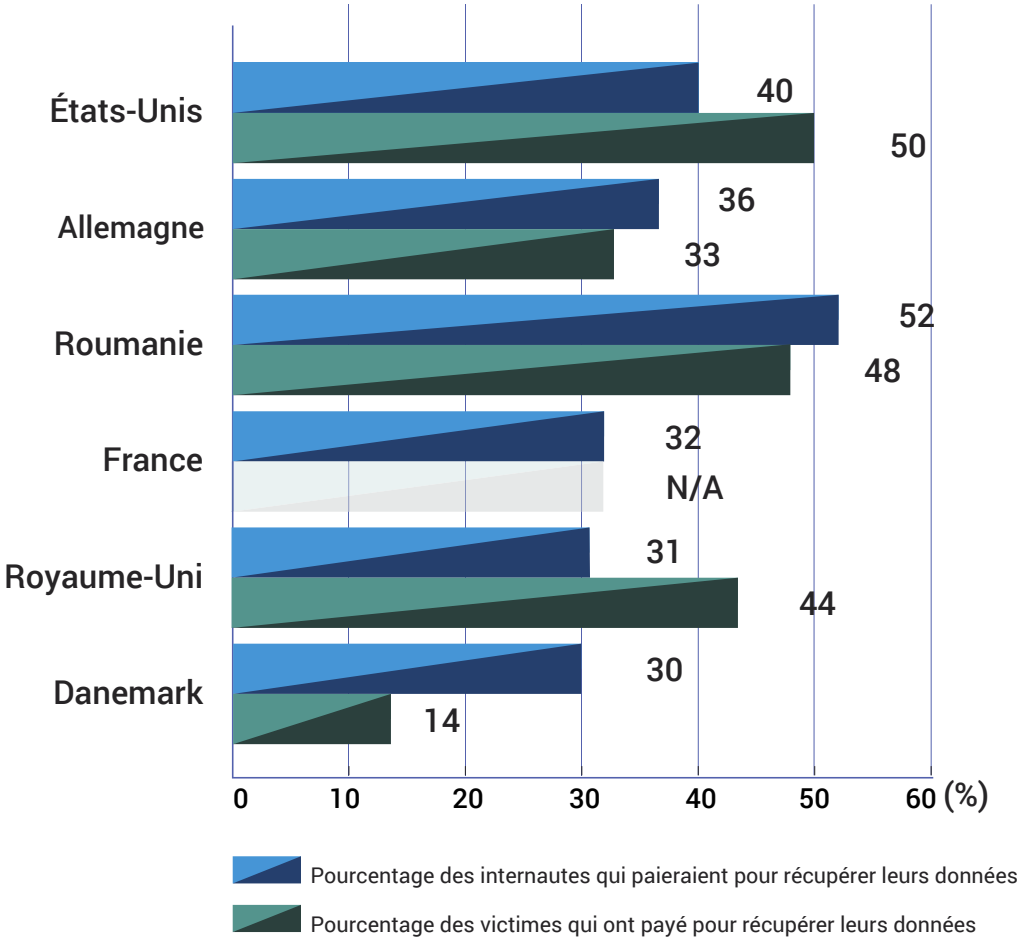
Les ransomwares rapportent donc énormément d'argent. Ces sommes sont ensuite réinjectées dans la cyber-criminalité.

[1] Tous les pourcentages incluent des sondés qui savent identifier un ransomware.

Les Américains sont plus enclins à sortir leur portefeuille

Aux États-Unis, plus de 50% des victimes de ransomwares ont payé les escrocs, ce qui montre qu'au moins une partie des données affectées avait de la valeur aux yeux des internautes.

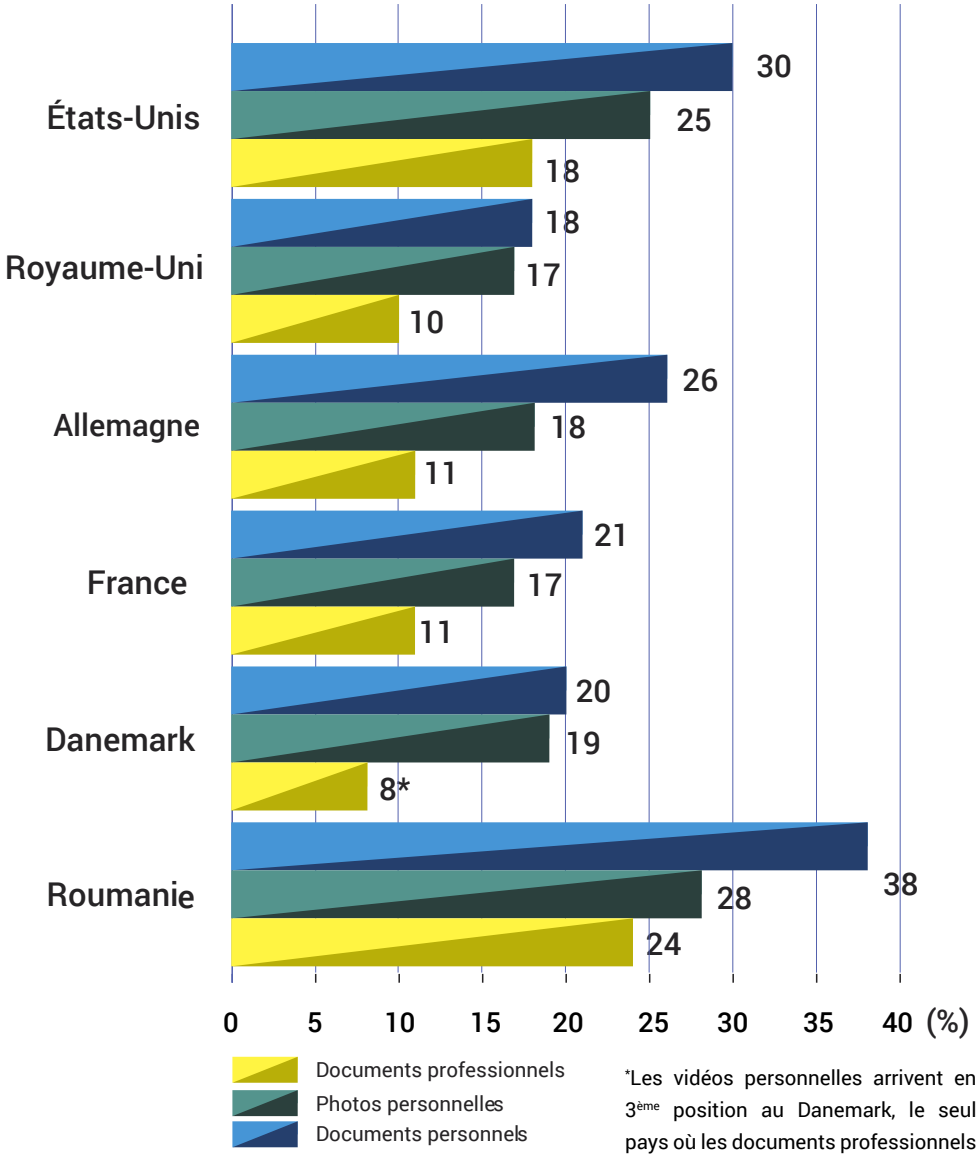
La Roumanie et le Royaume-Uni suivent cette tendance, car respectivement 48% et 44% des victimes ont payé une rançon après avoir été infectés. Les Allemands et les Danois sont plus réticents, car ils ne sont respectivement que 33% et 14% à avoir payé les sommes demandées.



Les photos personnelles ont une grande valeur

Lorsqu'on leur a demandé de classer le type de données par ordre d'importance, les personnes interrogées de nationalité américaine ont déclaré qu'elles donnaient plus de valeur aux documents personnels et à leurs photos. 30% paieraient pour récupérer leurs documents personnels et 25% pour leurs photos, tandis que 18% paieraient pour récupérer des documents liés à leur travail.

Chez tous les internautes sondés, certaines données sont plus importantes que d'autres ; le même ordre d'importance a été observé au Royaume-Uni, en Allemagne, en France, au Danemark et en Roumanie, différant seulement au niveau des pourcentages. Par exemple, 21% des sondés français paieraient pour des photos personnelles, et seulement 10% pour des documents professionnels.



*Les vidéos personnelles arrivent en 3ème position au Danemark, le seul pays où les documents professionnels arrivent 4ème.

Avec 26% des Allemands prêts à payer pour des documents personnels, seulement 18% paieraient pour des photos personnelles, et 11% pour des documents professionnels.

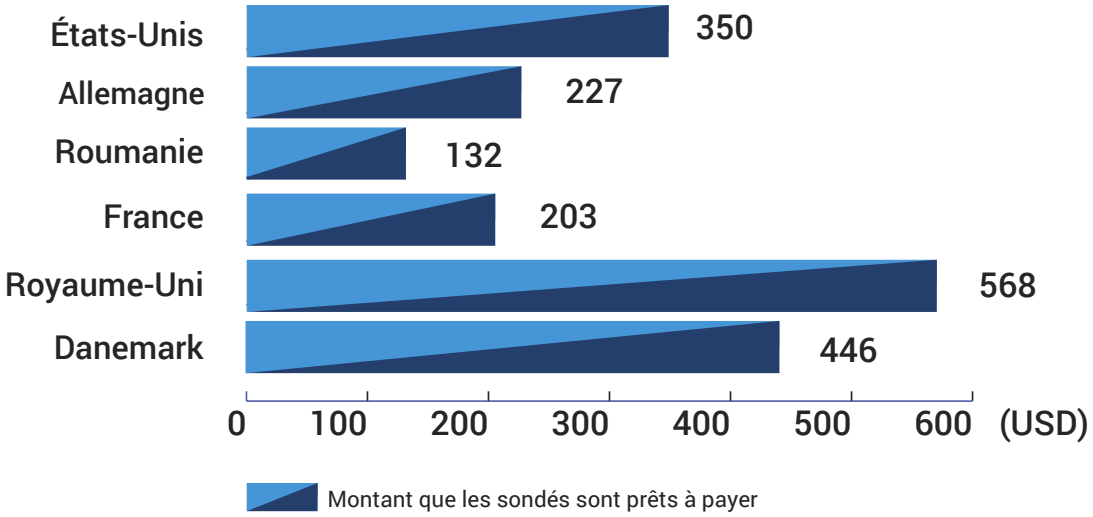
En Angleterre, au Danemark et en Roumanie, respectivement 18%, 20% et 38% des sondés considèrent que les documents personnels sont d'une importance capitale et paieraient pour les récupérer.

Les photos personnelles arrivent en seconde position par ordre d'importance en France, au Danemark et en Roumanie, avec respectivement 17%, 19% et 28% des sondés exprimant leur volonté de les récupérer. Les documents professionnels arrivent en 3ème position pour ces mêmes pays, avec seulement respectivement 11%, 8% et 24% des sondés. Seuls les Danois mettent leurs vidéos personnelles en 3ème place.

Les Britanniques payent plus cher

Les victimes britanniques sont enclines à payer plus pour récupérer leurs documents personnels, leurs photos et documents professionnels, donnant presque trois fois plus d'argent que les Français. En effet, les Britanniques sont prêts à payer près de 526 euros pour déchiffrer leurs fichiers tandis que les Français seraient prêts à donner "seulement" 188 euros pour récupérer leurs données. Quant aux Allemands, ils seraient prêts à verser jusqu'à 211 euros.

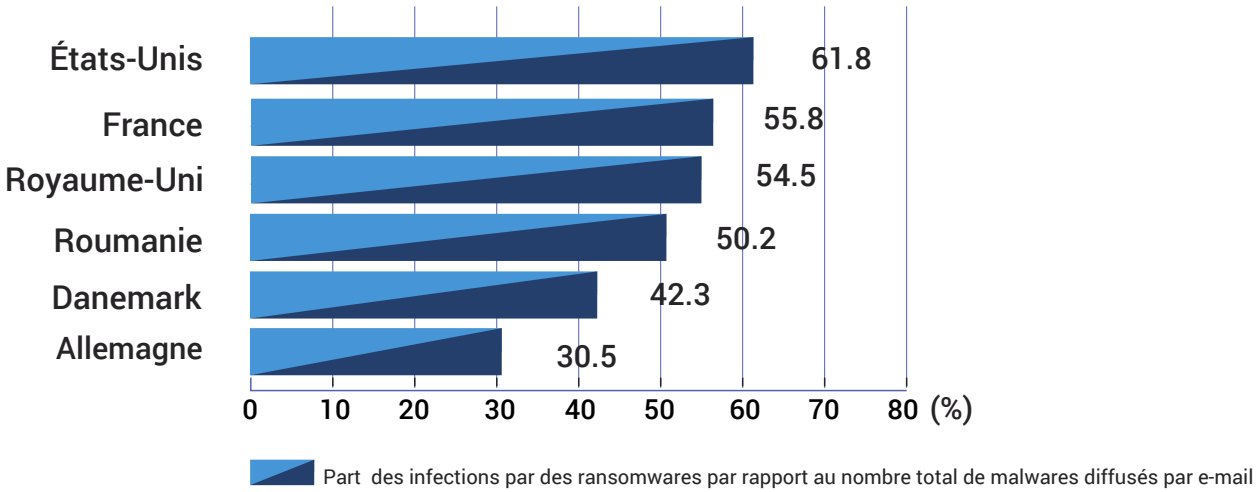
Les sondés américains et danois dépenseraient respectivement jusqu'à 350 dollars et 311 euros, tandis que les Roumains n'iraient pas au delà de 122 euros.



La peur des spams

Les rapports internes de Bitdefender montrent que 61,8% de tous les malwares distribués par e-mail ciblant les internautes américains sont des variantes de menaces ransomwares. La France se classe en deuxième position avec 55,8% tandis que le Royaume-Uni, la Roumanie, le Danemark et l'Allemagne obtiennent respectivement un résultat de 54,5% 50,2%, 42,3% et 30,5%.

Alors que les e-mails contiennent aussi d'autres menaces, telles que des chevaux de Troie, des spywares et keyloggers, ils semblent constituer le vecteur principal pour diffuser des infections par des ransomwares. Afin d'attiser la curiosité de l'internaute, les e-mails affichent un message du type « Veuillez trouver ci-joint », « Ci-joint votre facture » ou « Voici votre suivi de colis ».



Qui sont les plus ciblés ? Il s'agit des internautes américains. 21,21% de tous les e-mails infectés par des ransomwares dans le monde ciblent les États-Unis. Le Royaume-Uni et la France arrivent en seconde et troisième position avec 9,1% et 3,85%.

La Roumanie, l'Allemagne et le Danemark ne pèsent respectivement que 3,46%, 3,4% et 0,10% des e-mails contenant des ransomwares, probablement parce que les cybercriminels pensent que les utilisateurs américains sont plus enclins à payer.

9 utilisateurs de réseaux sociaux sur 10 affirment que les attaques peuvent se produire à n'importe quel moment.

Précisions sur l'étude :
L'étude a été conduite en novembre 2015 sur 3009 personnes en Roumanie, aux États-Unis, au Royaume-Uni et en Irlande du Nord, en France, en Allemagne, et au Danemark. La marge d'erreur pour le Royaume-Uni est de ± 4,38%. La marge d'erreur pour le Danemark, l'Allemagne, et les États-Unis est de ± 3,1%, tandis que pour la France et la Roumanie, elle est de ± 6,88%. L'intervalle de confiance est de 95%.

Dans la plupart des pays sondés, la majorité des personnes interrogées sont des hommes (52%), entre 36 et 55 ans. Au Royaume-Uni et en France, la proportion de femmes est légèrement plus importante, tandis qu'en Allemagne et au Danemark le nombre d'hommes et de femmes est identique. La moitié des sondés sont des managers, avec un bac +5 et mariés avec des enfants.

2ème PARTIE
Zoom sur les ransomwares

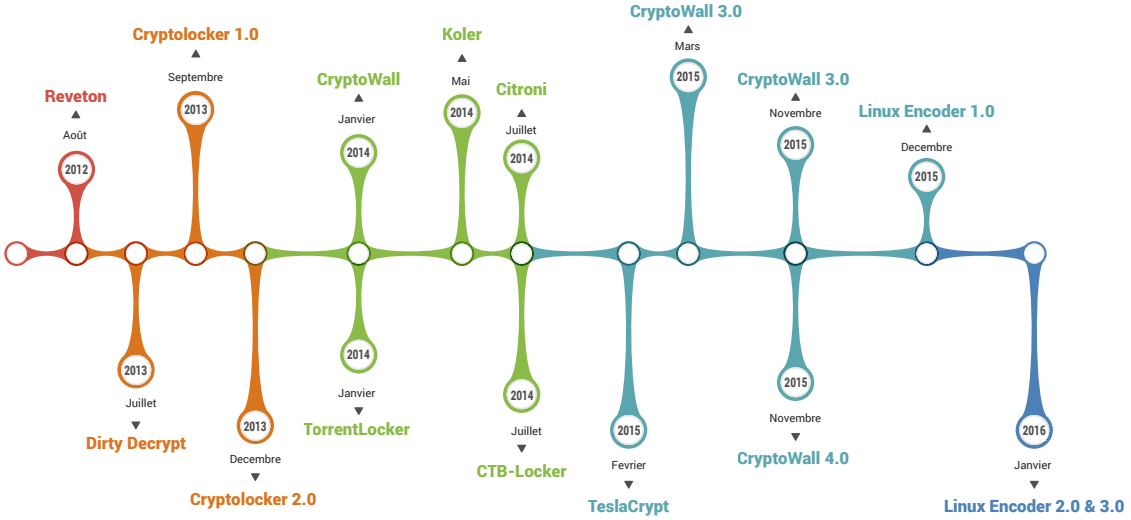
Le ransomware de dernière génération est un type de malware qui verrouille et généralement chiffre un système d'exploitation jusqu'à ce que l'utilisateur finisse par payer pour y avoir de nouveau accès. Le malware peut pénétrer un système via un fichier malveillant téléchargé, un e-mail ou un SMS.

En quoi est-il différent des malwares traditionnels ?

- Il ne vole pas les données des victimes, mais les chiffre.
- Il n'a pas besoin de se cacher une fois les fichiers chiffrés, car sa suppression ne permettra pas la récupération des données perdues.
- Il demande une rançon, généralement en devise virtuelle (par exemple en Bitcoin).
- Il est relativement facile à créer : il existe des bibliothèques de chiffrement (crypto-librairies) bien documentées.

Types connus

L'extorsion n'est pas une pratique nouvelle, mais cette menace n'a fait son apparition dans le monde numérique qu'à partir des années 2000, en se cachant dans un outil de suppression de spywares : ce dernier exagérait les problèmes présents sur l'ordinateur, tels que les entrées de registre non utilisées ou les fichiers corrompus et il affirmait pouvoir les résoudre si l'utilisateur acceptait de payer entre 27 et 80 euros. Une étape fut franchie entre 2008 et 2009, lorsque les cybercriminels commencèrent à créer de faux programmes antivirus, une pratique encore plus trompeuse et agressive. En 2011, les attaquants sont passés des faux antivirus, également appelés "Rogue" à une forme d'extorsion plus sophistiquée : les virus chiffrant les fichiers.

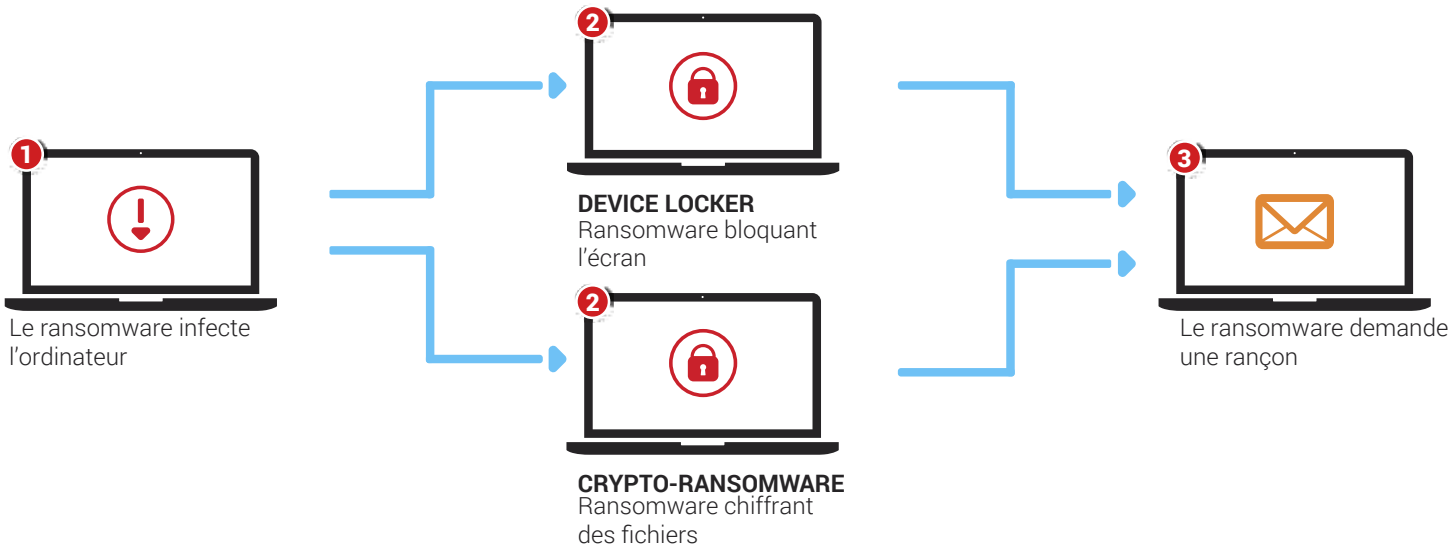


On trouve aujourd'hui deux formes principales de ransomwares en circulation :

Les device lockers. Ces ransomwares verrouillent l'écran et affichent une image en plein écran qui bloque l'accès à l'appareil. Ce message demande une rançon mais les fichiers personnels ne sont pas chiffrés. Ce type de ransomware prend souvent la forme d'un message de la police et menace l'utilisateur d'une amende pour ses prétendues activités douteuses ou criminelles en ligne.

Les crypto-ransomwares. Ces ransomwares chiffrent les données des utilisateurs. Le chiffrement de fichiers est bien plus évolué que le verrouillage d'écran, allant jusqu'à un chiffrement irréversible, rendant les documents, fichiers, photos et vidéos inaccessibles à moins de disposer de la clé de déchiffrement.

Ces deux types de malwares empêchent l'accès à ce que contient l'ordinateur, mais les verrouilleurs d'écran peuvent être contournés via différentes techniques et outils de récupération, tandis que le chiffrement est bien plus difficile à décoder, le rendant destructeur par nature.



Comment la chaîne d'infection opère-t-elle ?

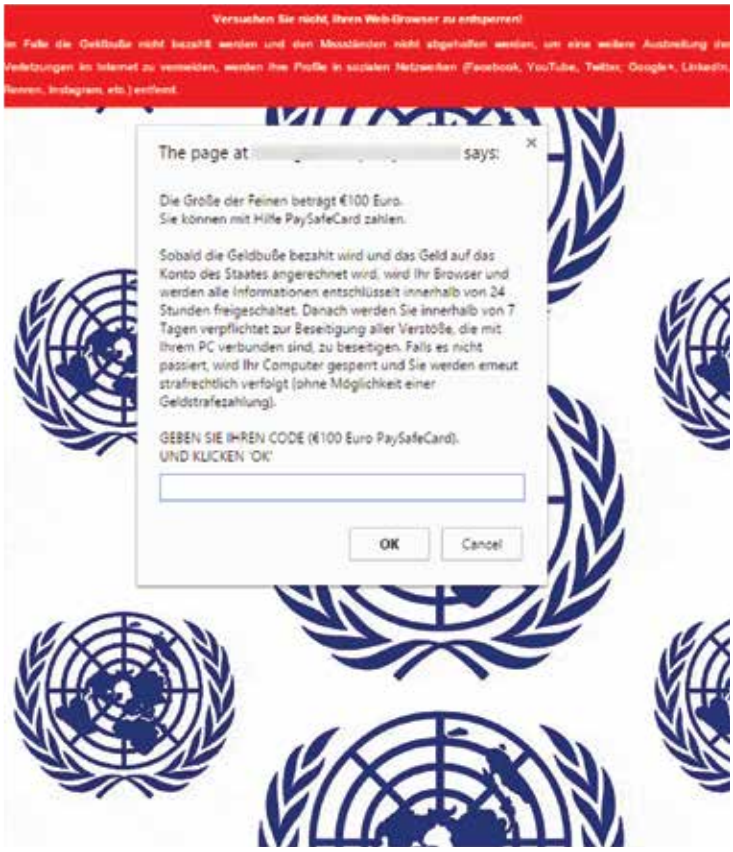
Le ransomware prolifère via ces principaux vecteurs d'attaque :

- Le spam et l'ingénierie sociale
- Le drive-by-download direct
- Le drive-by-download via publicité
- Les outils d'installation de malwares et les botnets

Après avoir infiltré la machine, le crypto-ransomware se connecte à des domaines générés aléatoirement pour récupérer une clé de chiffrement. Il cherche ensuite du contenu appartenant à l'utilisateur, tel que des documents (.doc, .xls), des présentations (.pdf, .ppt), des photos (.jpg) et autres extensions de fichiers. Par exemple, CryptoLock est capable de chiffrer plus de 70 types de fichiers. Une fois les fichiers ciblés identifiés, une clé sera générée pour chaque fichier et utilisée pour chiffrer les données, selon des algorithmes de chiffrement plus ou moins complexes. Le processus rend les données inutilisables.

Le malware affiche un message informant les victimes que pour récupérer leurs données, ils doivent payer rapidement via des devises virtuelles ou un coupon prépayé, avant une date limite. La victime procède alors au paiement et envoie une confirmation. Une fois la transaction terminée, les pirates envoient la clé de déchiffrement.

Il arrive que les cybercriminels traduisent les messages qui s'affichent pour que les messages aux victimes soient plus clairs.



Le développement du ransomware et ses évolutions pour 2016

Les ransomwares sous Android

Alors que les ransomwares ont proliféré sur Windows pendant plusieurs années, les cybercriminels ont désormais des vues sur de nouvelles plateformes. Le système d'exploitation Android est considéré comme le plus susceptible d'être touché par cette nouvelle génération de ransomware. En effet, avec plus de 1,4 milliard d'utilisateurs dans le monde, selon le PDG de Google Sundar Pichai, et une part de marché impressionnante de 82.2% au 2ème trimestre de 2015, selon IDC, Android est une cible idéale.

La plupart des ransomwares sur Android sont des device lockers ; ils bloquent le smartphone et affichent un message demandant une rançon, sans chiffrer les données. Même si certains sont capables de chiffrer la carte SD, les variantes les plus fréquentes en 2015 tentaient avant tout d'effrayer les utilisateurs pour qu'ils cèdent à leurs demandes.

Une variante de malware sur Android est ainsi capable de changer le code PIN de l'appareil, tout en arrêtant tout processus de sécurité afin d'éviter d'être détecté. Ce comportement, similaire à ce qu'on peut trouver sur PC, signifie que de nouvelles fonctionnalités risquent d'arriver rapidement en 2016.

En ce qui concerne les vecteurs d'infection, l'une des méthodes les plus communes pour installer un ransomware Android sont les publicités malveillantes ; les cybercriminels achètent des espaces publicitaires sur des sites Web légitimes et diffusent des publicités infectées. En cliquant sur ces publicités, les internautes sont redirigés vers de fausses boutiques en ligne, ou sont incités à télécharger de faux lecteurs vidéo ou de fausses mises à jour.

De plus, Google ayant autorisé l'obfuscation du code en développant l'outil ProGuard, l'analyse et la détection de menaces sur Android vont devenir encore plus complexes, ce qui va permettre à ces menaces de proliférer sur des stores, y compris le Google Play Store.

Les statistiques internes de Bitdefender concernant Android montrent que la famille du ransomware Android SLocker représentait plus de 4,35% des infections au cours du 3ème trimestre 2015 et 3,08% au cours du dernier trimestre 2015.

Les ransomwares dans les navigateurs

Bien qu'encore assez rares en 2015, les ransomwares dans les navigateurs sont une méthode efficace pour forcer les victimes à payer. Constituant l'un des types de ransomwares les plus simples, il empêche les utilisateurs de changer d'onglets dans leur navigateur tout en affichant une fausse amende pour navigation illégale sur des sites pornographiques.

Parce qu'il n'y a aucun malware réellement installé sur l'appareil et qu'il s'agit uniquement d'un JavaScript qui empêche les onglets d'être fermés, le ransomware de navigateur est assez simple à supprimer. Néanmoins, le fait qu'il soit codé en JavaScript le rend multiplateforme. Il peut donc toucher tous les utilisateurs, qu'ils utilisent Windows, Mac OS X, Android ou autre.

Les ransomwares sous Linux

Les dernières évolutions ont permis aux ransomwares de viser Linux. Les cybercriminels souhaitent viser cette plateforme car les serveurs Web sous Linux sont le cœur-même d'Internet, de nombreux serveurs hébergeant plusieurs dizaines de sites Web. Une infection réussie pourrait alors affecter de nombreuses victimes à la fois et donc permettre une augmentation des revenus générés par les rançons.

Jusqu'ici les tentatives de création d'une forme persistante de ransomware sous Linux ont échoué, car les chercheurs de Bitdefender ont pu trouver des failles dans les algorithmes de chiffrement utilisés pour chiffrer les données et ainsi fournir un outil de déchiffrement gratuit pour récupérer les fichiers Linux chiffrés par Linux.Encoder.

Exploitant surtout les vulnérabilités dans Joomla ou d'autres composants non patchés de Linux, un ransomware sous Linux qui fonctionne correctement aurait un effet tout à fait dévastateur sur Internet, car les serveurs Web qui forment la plus grande partie d'Internet s'appuient sur Linux pour livrer des millions de pages Web aux utilisateurs. L'une de nos prédictions pour 2016 concerne l'évolution du ransomware sous Linux, le désignant comme l'une des menaces les plus sérieuses à prendre en compte.

L'évolution du chiffrement

Le ransomware sous Windows a beaucoup évolué ces dernières années pour faire face aux évolutions de la législation et au travail des entreprises spécialisées dans la cyber-sécurité qui ont œuvré à contrer les variantes les plus répandues, telles que CryptoLocker, TorLocker, BitLocker et autres.

Non seulement les cybercriminels ont intégré des mécanismes de polymorphisme et d'obfuscation à ces variantes, mais les mécanismes de chiffrement ont également évolué, ce qui rend la localisation de leurs serveurs ainsi que le déchiffrement des fichiers encore plus difficiles.

À cette fin les premiers échantillons de ransomware utilisaient un chiffrement asymétrique (RSA), nécessitant des clés à la fois publiques et privées pour déchiffrer les données. Bien évidemment, les clés de déchiffrement privées étaient stockées sur des serveurs C&C (Command & Control) et envoyées aux victimes uniquement après qu'elles aient accepté de payer la rançon.

Afin de rendre l'authentification des serveurs C&C encore plus difficile, les pirates utilisent le réseau Tor (The Onion Router), pour rendre anonyme l'adresse du domaine du serveur. Alors que le réseau Tor a été créé dans le but d'assurer une navigation Web sécurisée pour tout le monde, ce sont ceux qui ne souhaitaient pas être suivis (les cybercriminels ou les cyber-terroristes) qui l'ont rapidement adopté.

Les ordinateurs infectés sous Windows communiquent donc avec les serveurs via TOR, ce qui complique le processus de démantèlement par les autorités et les entreprises spécialisées dans la cyber-sécurité.

Les ransomwares ont choisi une tactique extrêmement intéressante quand ils ont commencé à cibler les systèmes d'exploitation Linux, en chiffrant des fichiers stockés sur les serveurs Web, tels que les pages Web. Si les trois premières variantes de Linux.Encoder ont permis aux chercheurs Bitdefender de deviner facilement la clé de chiffrement et de fournir un outil de déchiffrement gratuit pour les victimes, il devient de plus en plus évident que les cybercriminels essayent de renforcer le chiffrement afin d'éviter que ce contournement soit possible.

Le modèle économique du ransomware

Le mystérieux « Dark Web » est une partie du Web associée aux activités criminelles, cybercriminelles et même terroristes, alimentant les trafics illégaux en tous genres, de la drogue, aux armes, voire même jusqu'au meurtre. Les hackers et d'autres criminels y proposent leurs services sur le Web sous forme d'enchères et peuvent développer des malwares personnalisés contre de grosses sommes – généralement payées en monnaie virtuelle comme le Bitcoin.
[10]

Le "Malware-As-A-Service" a aussi vu le jour. Des hackers ont par exemple mis en place un système de kit de ransomware. Ces kits, moyennant 2 700 euros, permettent à n'importe qui de créer sa propre variante de ransomware et de gagner de l'argent via des rançons. Avec un retour sur investissement attendu assez rapide à condition de disposer d'une base de diffusion conséquente, ces tarifs sont particulièrement incitatifs pour ceux qui sont prêts à enfreindre la loi.

Le kit de CryptoLocker/Cryptowall a été repéré en vente pour ce montant. Ses développeurs proposent même des "business models" allant de l'affiliation (où le client et les développeurs se partagent les montants récoltés) jusqu'au partenariat, pouvant mener aussi vers d'autres activités cybercriminelles.

En plus d'acheter le code source complet du malware et sa capacité à générer de nouveaux échantillons, le client dispose aussi d'un support disponible 7j/7, 24h/24.

Les activités cybercriminelles sur le Dark Web connaissent une évolution constante. Le modèle Malware-As-A-Service est quant à lui, proche des services en ligne proposés légalement.

Les ransomwares paralysent les entreprises

Bitdefender prédit que les ransomwares vont intensifier leurs attaques contre les petites et moyennes entreprises.

En plus des capacités de chiffrement des fichiers, les ransomwares peuvent contenir des fonctionnalités ressemblant à celles des vers. Il suffit alors d'infecter un seul poste pour pouvoir contaminer tout le réseau d'une entreprise. En touchant ainsi des ordinateurs de bureau, des portables, des serveurs de données, le ransomware est alors capable de paralyser entièrement une petite entreprise.

En plus d'offrir la possibilité de pouvoir toucher un plus grand nombre de postes, les entreprises sont bien plus enclines à payer pour récupérer leurs données que les particuliers. La monétisation et la profitabilité ont toujours été les préoccupations principales des cybercriminels. En 2016, ils vont probablement atteindre des taux historiques grâce au ciblage des petites et moyennes entreprises.

La protection pour les particuliers et les entreprises

Une façon efficace de se protéger pour un particulier ou une entreprise est l'utilisation d'une solution de sécurité qui peut identifier rapidement les Menaces et atténuer la portée des infections.

Voici quelques étapes à suivre pour se protéger efficacement contre les ransomwares :

- Utiliser une suite de sécurité connue et primée pour sa protection et ses performances.
- Mettre régulièrement à jour le système d'exploitation et les logiciels pour éviter des failles de sécurité.
- Sauvegarder ses données personnelles.
- Désactiver l'option « Masquer l'extension des fichiers ». Cela aidera à identifier des exécutables se faisant passer pour des archives zip.

En ce qui concerne les entreprises :

- Utiliser une solution de sécurité pour Endpoint.
- Mettre à jour régulièrement les solutions pour Endpoint ainsi que les serveurs.
- Déployer une solution de sauvegarde.
- Empêcher les fichiers de s'exécuter dans des endroits critiques tels que "AppData/LocalAppData" et déployer des politiques empêchant l'exécution des fichiers inconnus.
- Limiter l'accès aux disques réseaux.
- Protéger les serveurs e-mails avec des solutions antispam et de filtrage de contenu.
- Former les employés à identifier les e-mails malveillants et les autres techniques d'ingénierie sociale.

Bitdefender propose des technologies de sécurité dans plus de 100 pays via un réseau de partenaires de premier plan, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.

PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender

Bitdefender

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.